

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-012123

(43)Date of publication of application : 16. 01. 2001

(51)Int. CI.

E05B 49/00

B60R 25/04

F02D 29/02

F02D 45/00

F02N 15/00

(21)Application number : 11-183808

(71)Applicant : ASAHI DENSO CO LTD

(22)Date of filing : 29. 06. 1999

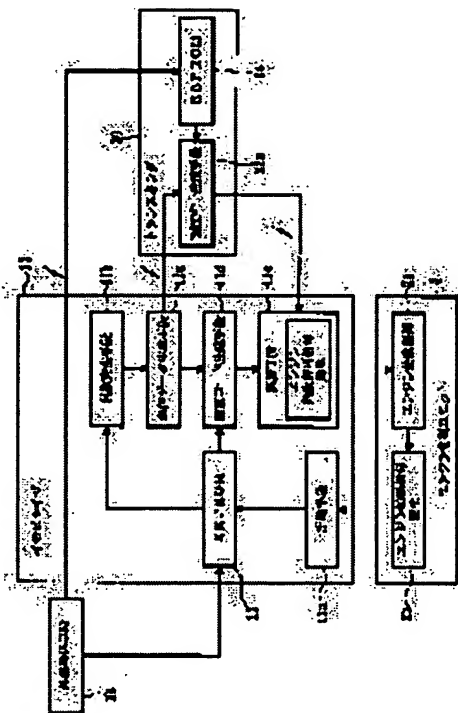
(72)Inventor : SUZUKI MICHIOYUKI

(54) IMMOBILIZER, AND ATTESTING METHOD BY IMMOBILIZER

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an immobilizer which is high in reliability of attestation, surely antitheft for a vehicle with its engine stopped, preventive from any misoperation, easy in fitting, and particularly effective for motorcycles, and an attestation method by the immobilizer.

SOLUTION: The random number data is generated based on the engine starting time data stored in a storage means, the random number data is transmitted to a transponder 20 through a radio part, the key specific information is coded using a specified coding method based on the random number data to generate the attestation code, the transponder 20 receives a generated attestation key in which the key specific information is coded using the coding method based on the random number data, an engine start permission signal is transmitted to an engine control unit 2 when the attestation code matches with the attestation key, and the time until the engine is started after a power source for an immobilizer 10 is turned on is stored in the storage means.



LEGAL STATUS

[Date of request for examination]

13. 11. 2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

from
CSP-III-A

[Date of extinction of right]

Copyright (C); 1998, 2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-12123

(P2001-12123A)

(43) 公開日 平成13年1月16日 (2001.1.16)

(51) Int. Cl.	識別記号	F I	ページ (参考)
E 0 5 B 49/00		E 0 5 B 49/00	K 2 E 2 5 0
B 6 0 R 25/04	6 1 0	B 6 0 R 25/04	6 1 0 3 G 0 8 4
F 0 2 D 29/02		F 0 2 D 29/02	K 3 G 0 9 3
45/00	3 4 5	45/00	3 4 5 L
F 0 2 N 15/00		F 0 2 N 15/00	F
審査請求 未請求 請求項の数 6 O L (全 14 頁)			

(21) 出願番号 特願平11-183808

(22) 出願日 平成11年6月28日 (1999. 6. 29)

(71) 出願人 000213654

朝日電装株式会社

静岡県浜北市中桑1126番地

(72) 発明者 鈴木 通之

静岡県浜北市中桑1126番地 朝日電装株式会社内

(74) 代理人 100095614

弁理士 越川 隆夫

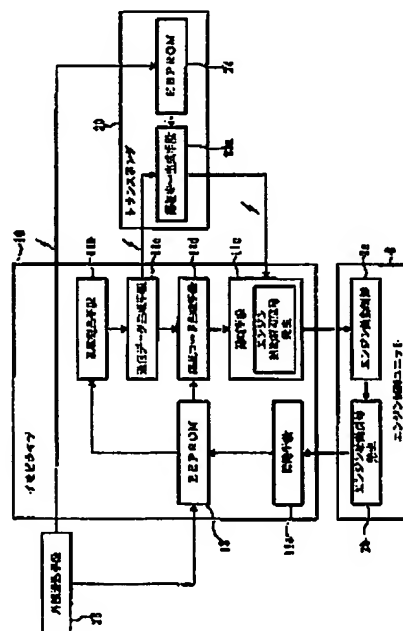
最終頁に続く

(54) 【発明の名称】 イモバイザ及びイモバイザによる認証方法

(57) 【要約】

【課題】 認証の信頼性が高く、エンジン停止中の車両に対して確実な盗難防止が可能で、誤動作を防止できると共に装着が容易で、特に二輪車に有効なイモバイザ及びイモバイザによる認証方法を提供することにある。

【解決手段】 記憶手段に記憶されているエンジンの始動時間データを基に乱数データを生成し、無線部を介して乱数データをトランスポンダに送信すると共に、乱数データを基に所定の暗号化手法を用いてキーの固有情報を暗号化して認証コードを生成し、乱数データを基に該暗号化手法を用いてトランスポンダがキーの固有情報を暗号化した生成した認証キーを受信し、認証コードと認証キーとが一致したときに、エンジン制御ユニットにエンジン始動許可信号を送出し、イモバイザの電源オンから、エンジンが始動するまでの時間を始動時間データとして記憶手段に記憶することを特徴とする。



(2)

特開2001-12123

1

2

【特許請求の範囲】

【請求項1】車両用のキーに内蔵されたトランスポンダの情報を基に特定のキーを識別するイモビライザによる認証方法において、記憶手段にあらかじめ記憶されているエンジンの始動時間データを基に乱数データを生成し、次に、無線部を介して該乱数データを該トランスポンダに送信すると共に、該乱数データを基に、所定の暗号化手法を用いて該キーの固有情報を暗号化することにより認証コードを生成し、該乱数データを基に、該暗号化手法を用いて該トランスポンダが該キーの固有情報を暗号化することにより生成した認証キーを受信した後、該認証コードと該認証キーとが一致したときに、エンジン制御ユニットにエンジン始動許可信号を送出し、該イモビライザの電源オンから、該エンジンが始動するまでの時間を該始動時間データとして該記憶手段に記憶してなるイモビライザによる認証方法。

【請求項2】前記エンジンが始動した後、前記無線部を停止すると共に、前記イモビライザを休止してなる請求項1記載のイモビライザによる認証方法。

【請求項3】車両用のキーに内蔵されたトランスポンダの情報を基に特定のキーを識別するイモビライザによる認証方法において、記憶手段にあらかじめ記憶されている該イモビライザの電源オン時間データを基に乱数データを生成し、次に、無線部を介して該乱数データを該トランスポンダに送信すると共に、該乱数データを基に、所定の暗号化手法を用いて該キーの固有情報を暗号化することにより認証コードを生成し、該乱数データを基に、該暗号化手法を用いて該トランスポンダが該キーの固有情報を暗号化することにより生成した認証キーを受信した後、該認証コードと該認証キーとが一致したときに、エンジン制御ユニットにエンジン始動許可信号を送出し、イグニッションスイッチのオン/オフにより該イモビライザの電源のオン/オフを行い、該イモビライザの電源がオンされている時間を該電源オン時間データとして該記憶手段に記憶してなるイモビライザによる認証方法。

【請求項4】車両用のキーに内蔵されたトランスポンダの情報を基に特定のキーを識別するイモビライザにおいて、該イモビライザの電源オンから、エンジンが始動するまでの時間をカウントして始動時間データを生成する計時手段と、該始動時間データを記憶する記憶手段と、該記憶手段に記憶されている始動時間データを基に乱数データを生成する乱数発生手段と、該乱数データを基に、所定の暗号化手法を用いて該キーの固有情報を暗号化することにより認証コードを生成する認証コード生成手段と、該トランスポンダに該乱数データを送信すると共に、該乱数データを基に、該暗号化手法を用いて該トランスポンダが該キーの固有情報を暗号化することにより生成した認証キーを受信する無線部と、該認証コードと該認証キーとが一致したときに、該エンジン制御ユニ

ットにエンジン始動許可信号を送出する認証手段とを備え、該始動時間データを用いて該キーを認証することを特徴とするイモビライザ。

【請求項5】前記エンジンが始動した後、前記無線部を停止すると共に、前記イモビライザを休止することを特徴とする請求項4記載のイモビライザ。

【請求項6】車両用のキーに内蔵されたトランスポンダの情報を基に特定のキーを識別するイモビライザにおいて、イグニッションスイッチによりオン/オフする電源部と、該イモビライザの電源オン時間データを生成する計時手段と、該電源オン時間データを記憶する記憶手段と、該記憶手段に記憶されている電源オン時間データを基に乱数データを生成する乱数発生手段と、該乱数データを基に、所定の暗号化手法を用いて該キーの固有情報を暗号化することにより認証コードを生成する認証コード生成手段と、該トランスポンダに該乱数データを送信すると共に、該乱数データを基に、該暗号化手法を用いて該トランスポンダが該キーの固有情報を暗号化することにより生成した認証キーを受信する無線部と、該認証コードと該認証キーとが一致したときに、エンジン制御ユニットにエンジン始動許可信号を送出する認証手段とを備え、該イモビライザの電源オン時間を用いて該キーを認証することを特徴とするイモビライザ。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、自動二輪車や原動機付き自転車などの車両のキーに内蔵されたトランスポンダの情報を基に特定のキーを識別し、車両の盗難を防止するためのイモビライザ及びイモビライザによる認証方法に関する。

【0002】

【従来の技術】従来、車両の盗難を防止するためのイモビライザの一例として特開平11-91509号がある。同公報によれば、エンジン制御ユニットは、乱数を生成するシード生成手段と、乱数を外部へ送出するシード送信手段と、乱数を暗号化アルゴリズムにより暗号化して認証キーを生成する認証キー生成手段と、外部からキーを受信するキー受信手段と、外部からのキーと認証キーとを比較して、合致したときにセキュリティを解除する合致判定手段と、エンジンの回転数、燃料噴射量、吸入空気量、スロットル開度、水温、イグニッションスイッチのオン/オフ時のフリーランタイムの計時値などの車両制御情報を読み込む車両制御情報読み込み手段とを備えている。

【0003】また、ユーザー側キーユニットは、エンジン制御ユニットのシード送信手段からの乱数を受信するシード受信手段と、エンジン制御ユニットの認証キー生成手段と同一の暗号化アルゴリズムを有して、乱数を暗号化アルゴリズムにより暗号化してキーを生成するキー生成手段と、生成したキーをエンジン制御ユニットのキ

(3)

特開2001-12123

3

一受信手段へ送信するキー送信手段とを備えている。

【0004】エンジン制御ユニットでは、車両制御情報読み込み手段にてエンジンの回転数、燃料噴射量、吸入空気量、スロットル開度、水温などの車両制御情報を読み込み、シード生成手段にて複数の車両制御情報の加算値として乱数を生成する。ユーザー側キーユニットでは、エンジン制御ユニットから乱数を受信し、キー生成手段にてシード生成手段と同一の暗号化アルゴリズムによりキーを生成し、このキーをエンジン制御ユニットへ送信する。そして、エンジン制御ユニットの合致判定手段にて、ユーザー側キーユニットからのキーを認証キーと比較して、合致したときにセキュリティを解除する。

【0005】

【発明が解決しようとする課題】しかしながら、前記イモビライザにおいて、乱数を生成する基となる車両制御情報は、エンジンが動作している場合にのみ得られる情報であって、エンジン始動前に得られる情報ではない。このため、エンジンが動作していない車両に対するセキュリティ効果は有していない。

【0006】また、同公報には、エンジン停止後のセキュリティを確保するために、イグニッションスイッチのオン/オフ時のフリーランタイムの計時値を使用することが書かれている。しかしながら、計時値をどのように保持し使用するのかについての記載がない。

【0007】また、このイモビライザは、自動車のように、エンジンの回転数、燃料噴射量、吸入空気量、スロットル開度、水温などの高度な車両制御情報を収集している車両には適しているものの、原動機付き自転車のように、高度な車両制御情報を収集する必要のない車両においては、実用的ではない。

【0008】また、既に市販され使用されている車両に、このイモビライザのみを装着することは困難であり、エンジン制御ユニットを交換することとなり、多額の費用がかかってしまう。

【0009】本発明は、このような事情に鑑みてなされたもので、認証の信頼性が高く、エンジン停止中の車両に対して確実な盗難防止が可能で、誤動作を防止できると共に装着が容易で、特にエンジン制御ユニットが簡易な自動二輪車や原動機付き自転車などの二輪車に有効なイモビライザ及びイモビライザによる認証方法を提供することにある。

【0010】

【課題を解決するための手段】請求項1記載のイモビライザによる認証方法は、記憶手段にあらかじめ記憶されているエンジンの始動時間データを基に乱数データを生成し、次に、無線部を介して乱数データをトランスポンダに送信すると共に、乱数データを基に、所定の暗号化手法を用いてキーの固有情報を暗号化することにより認証コードを生成し、乱数データを基に、該暗号化手法を用いてトランスポンダがキーの固有情報を暗号化するこ

4

とにより生成した認証キーを受信した後、認証コードと認証キーとが一致したときに、エンジン制御ユニットにエンジン始動許可信号を送出し、イモビライザの電源オンから、エンジンが始動するまでの時間を始動時間データとして記憶手段に記憶することを特徴とする。

【0011】請求項2記載のイモビライザによる認証方法は、エンジンが始動した後、無線部を停止すると共に、イモビライザを休止することを特徴とする。

【0012】請求項3記載のイモビライザによる認証方法は、記憶手段にあらかじめ記憶されているイモビライザの電源オン時間データを基に乱数データを生成し、次に、無線部を介して乱数データをトランスポンダに送信すると共に、乱数データを基に、所定の暗号化手法を用いてキーの固有情報を暗号化することにより認証コードを生成し、乱数データを基に、該暗号化手法を用いてトランスポンダがキーの固有情報を暗号化することにより生成した認証キーを受信した後、認証コードと認証キーとが一致したときに、エンジン制御ユニットにエンジン始動許可信号を送出し、イグニッションスイッチのオン/オフによりイモビライザの電源のオン/オフを行い、イモビライザの電源がオンされている時間を電源オン時間データとして記憶手段に記憶することを特徴とする。

【0013】請求項4記載のイモビライザは、イモビライザの電源オンから、エンジンが始動するまでの時間をカウントして始動時間データを生成する計時手段と、始動時間データを記憶する記憶手段と、記憶手段に記憶されている始動時間データを基に乱数データを生成する乱数発生手段と、乱数データを基に、所定の暗号化手法を用いてキーの固有情報を暗号化することにより認証コードを生成する認証コード生成手段と、トランスポンダに乱数データを送信すると共に、乱数データを基に、該暗号化手法を用いてトランスポンダがキーの固有情報を暗号化することにより生成した認証キーを受信する無線部と、認証コードと認証キーとが一致したときに、エンジン制御ユニットにエンジン始動許可信号を送出する認証手段とを備え、始動時間データを用いてキーを認証することを特徴とする。

【0014】請求項5記載のイモビライザは、エンジンが始動した後、無線部を停止すると共に、イモビライザを休止することを特徴とする。

【0015】請求項6記載のイモビライザは、イグニッションスイッチによりオン/オフする電源部と、イモビライザの電源オン時間データを生成する計時手段と、電源オン時間データを記憶する記憶手段と、記憶手段に記憶されている電源オン時間データを基に乱数データを生成する乱数発生手段と、乱数データを基に、所定の暗号化手法を用いてキーの固有情報を暗号化することにより認証コードを生成する認証コード生成手段と、トランスポンダに乱数データを送信すると共に、乱数データを基に、該暗号化手法を用いてトランスポンダがキーの固有

(4)

特開2001-12123

5

5

情報を暗号化することにより生成した認証キーを受信する無線部と、認証コードと認証キーとが一致したときに、エンジン制御ユニットにエンジン始動許可信号を送出する認証手段とを備え、イモビライザの電源オン時間を用いてキーを認証することを特徴とする。

【0016】

【発明の実施の形態】以下、本発明の形態について図面を参照しながら具体的に説明する。図1、図3及び図4は第1の実施例を示す図面、図5～図7は第2の実施例を示す図面である。尚、図2は、第1の実施例と第2の実施例に共通する図面である。

【0017】（実施の形態1）図1は本発明のイモビライザの第1の実施例を示す構成図、図2は本発明のトランスポンダの一実施例を示す構成図である。図3は図1のイモビライザの動作の様子を示す構成図である。図4は図1のイモビライザの動作を示すフローチャートである。

【0018】図1～図4において、イモビライザ10は、自動二輪車や原動機付き自転車などの車両のキー3に内蔵されたトランスポンダ20との間で無線通信を行い、トランスポンダ20から送られる情報を基に、キー3がその車両固有のものであるかどうか識別し、車両の盗難を防止するための装置である。イモビライザ10は、CPU（central processing unit）11、電源部12、EEPROM（Electrically Erasable and Programmable Read Only Memory）13、通信インターフェース14、無線部15により構成されている。

【0019】CPU11は中央演算装置であって、イモビライザ10の動作を制御するものである。電源部12は、イモビライザ10が動作するための直流電源であるVDD17を、バッテリー7から作り出すためのものである。尚、バッテリー7は、キーシリンダ4内に設けられたイグニッションスイッチ5を介して電源部12に接続されている。このイグニッションスイッチ5は、キー3をキーシリンダ4に挿入して運転位置に回転セットしたときにオンとなるスイッチである。EEPROM13は、CPU11に接続された記憶手段であり、不揮発性である。尚、この実施の形態1については、EEPROM13を記憶手段として使用しているが不揮発性の記憶手段であればこれに限られるものではなく、例えば、EPROM（Erasable and Programmable Read Only Memory）、OTP（One Time Programmable read only memory）、フラッシュEEPROM、その他電源バックアップ機能付きのメモリ等が使用可能である。

【0020】通信インターフェース14は、CPU11とエンジン制御ユニット2とが通信するための仲介役であり、両者間の信号レベルや信号形式を整合させるものである。本実施の形態1においては、車両のエンジンの始動や停止を制御するためエンジン制御ユニット2と通信インターフェース14との間の通信は、シリアル信号

（例えばRS-232C準拠の信号）を使用している。これは、エンジン制御ユニット2に送る情報を複雑にし、外部から解読しにくくするためである。しかしながら、これに限られるものではなく、レベルの高低だけの1/O信号であっても差し支えない。尚、CPU11と通信インターフェース14とはバスにより接続されている。

【0021】無線部15は、CPU11から送られてくる情報を変調するものであり、変調された無線信号は、キーシリンダ4に内蔵されたアンテナ6からトランスポンダ20のアンテナ25に送られる。また、無線部15は、トランスポンダ20から送信された無線信号を、アンテナ6で受信して復調し、復調した情報をCPU11に送る。無線部15とVDD17の間には、無線部電源スイッチ16が設けられており、CPU11の指令により、無線部15の電源はオン/オフ可能となっている。

【0022】トランスポンダ20は、イモビライザ10から送られる無線信号を基に動作し、その無線信号に対しての回答となる信号を無線信号としてイモビライザ10に送信するものである。トランスポンダ20は、キー3に内蔵されている。トランスポンダ20は、イモビライザ10から送られる無線信号を受信したり、トランスポンダ20側で生成した情報を送信するためのアンテナ25、無線信号を変復調するための無線部22、トランスポンダ20の制御を行う認証キー生成IC23、車両固有の情報を格納する不揮発性の記憶手段であるEEPROM24と2次電池に相当するコンデンサ21から構成される。

【0023】次に、イモビライザ10の動作を説明する。尚、以下の説明において、括弧内の符号は図4のフローチャートの符号に対応している。運転者がキー3を用いて車両を始動させようとする場合は、まず、運転者はキー3をキーシリンダ4に挿入する。そして、キー3を運転位置（オン位置）に回す。すると、イグニッションスイッチ5がオンして、電源部12にバッテリー7が接続される。そして、VDD17が電源部12から出力され、イモビライザ10が動作を開始する。

【0024】イモビライザ10が動作を開始すると、まず最初に、CPU11はソフトウェアで実現されている計時手段11aによりイモビライザ10が動作している時間の計時を開始する（S100）。つぎに、エンジンが動作しているかを、エンジン制御ユニット2からエンジン始動信号線2sを介して送られるエンジン始動信号により確認する（S101）。キー3挿入当初はエンジンは始動していないので、CPU11はEEPROM13に格納されている始動時間データを読み出す（S102）。尚、始動時間データは、イモビライザ10の動作開始からエンジン始動までの時間を計時手段11aで計時して生成したデータであり、前回エンジンを始動させ

(5)

特開2001-12123

7

8

て時の始動時間データが、あらかじめEEPROM13に記憶されている。始動時間データの生成のタイミング等は後述する。また、車両を生産して初めてエンジンを始動させる時点でEEPROM13に記憶されているデータは、時間0のデータである。

【0025】次に、CPU11は乱数発生手段11bにより、読み出した始動時間データを基に、乱数データを発生させる(S103)。発生させる乱数データの大きさは、例えば10桁である。そして、CPU11は送信データ生成手段11cにより、無線部15からトランスポンダ20に送信するための送信データを生成する(S104)。この送信データ生成手段11cを介することなく、乱数データを直接無線部15から送信させることは可能である。しかしながら、本実施の形態1においては、乱数データに車種を限定するための情報を付加して、送信データを生成している。すなわち、例えば車種を限定するための2桁のパスワードを乱数データの先頭に付け加えている。パスワードの機能・効果については後述する。そして、生成された送信データを無線部15からトランスポンダ20に送信する(S105)。

【0026】トランスポンダ20側では、イモビライザ10からの送信データをアンテナ25を介して無線部22で受信する(S151)。無線部22で復調されたパスワード+乱数データを基に、認証キー生成IC23内の認証キー生成手段23aにより、認証キーを生成する(S152)。認証キーは、EEPROM24に記憶されているキー3固有の情報である暗号キーを用いて、乱数データを暗号化したもので、例えば、24ビットのデータである。尚、暗号化の方法は特に限定されるものではなく、例えばDES(Data Encryption Standard; 1977年米国商務省標準局が制定)等の方式が使用可能である。トランスポンダ20は、生成した認証キーを無線部22及びアンテナ25を介してイモビライザ10に送信する(S153)。

【0027】トランスポンダ20の認証キー生成手段23aは、イモビライザ10の情報を受信するとすぐに動作するのではなく、まず、パスワードの内容が、認証キーの生成を行ってもよいものであるかを確認する。当然、不正なパスワードであったり、パスワードがはじめから含まれていない場合には、トランスポンダ20は認証キーの生成及び送信を行わない。このように、トランスポンダ20側からの認証キーの発信を制限することで、このキー3が他車種のイモビライザに接近した場合に、不必要な信号を発信しないようにすることができ、複数のキーを1つのキーホルダに兼ねている場合などに、他車両の正規な認証に誤信を与えるのを防止可能である。

【0028】トランスポンダ20は電池を有しておらず、イモビライザ10の無線部15から、パスワード+乱数データの前に送られる電力信号により、無線部22

を動作させると共に、コンデンサ21を帯電する。すなわち、コンデンサ21は、イモビライザ10の無線部15から送られる電力信号により、2次電池として充電され、トランスポンダ20を動作させる。

【0029】トランスポンダ20が認証キーを生成している間に、イモビライザ10側では認証コードの生成を、CPU11の認証コード生成手段11dにおいて行う(S106)。認証コードは、パスワード+乱数データを基に、EEPROM13に記憶されているキー3固有の情報である暗号キーを用いて、乱数データを暗号化したものである。尚、暗号化の方式は、トランスポンダ20で使用されているものと同一のものである。

【0030】次に、イモビライザ10は、トランスポンダ20からの認証キーを受信する(S107)。そして、CPU11の認証手段11eにおいて、認証コードと認証キーの比較認証を行う(S108)。認証コードと認証キーとが一致した場合には、エンジン始動許可信号を発生する。このエンジン始動許可信号はCPU11から、通信インターフェース14を介して、エンジン制御ユニット2に送られる(S109)。エンジン始動許可信号を受信したエンジン制御ユニット2は、エンジン始動制御2aを行いエンジンを始動させる。実際の自動車や自動二輪車等においては、エンジン始動許可信号によりエンジン始動可能状態となり、運転者のスタータスイッチ(スタートスイッチ)のオンにより、エンジンの始動が行われる。エンジン制御ユニット2は、エンジンの始動を確認すると、イモビライザ10に対して、エンジン始動信号発生2bを行う。

【0031】イモビライザ10は、あらためてエンジン始動を確認する(S101)。ここで、エンジンの始動を確認すると、計時手段11aによる始動信号の計時を終了し、計時した始動時間データをEEPROM13に書き込み、前回始動時のデータを更新する(S111)。更新の方法としては、EEPROM13にすでに書き込まれている始動時間データに新たな始動時間データを足し合わせて新たな始動時間データを生成してもよいし、新たな始動時間データを前回の始動時間データと置き換えてしまってもよい。

【0032】次に、CPU11は無線部電源スイッチ16をオフして、無線部15を停止させる(S112)。そして、一連のキー認証作業を終えた後に、CPU11を休止状態にすることにより、イモビライザ10を休止させる(S113)。

【0033】尚、本実施の形態1においては、始動時間の計時の開始をイモビライザ10の動作開始時としているが、計時開始をイモビライザ10がエンジン始動許可信号を出力した時としてもよい。

【0034】また、本実施の形態1において、計時手段11a、乱数発生手段11b、送信データ生成手段11c、認証コード生成手段11d及び認証手段11eは、

(5)

特開2001-12123

9

10

CPU11によりソフトウェアとして実現されている。しかしながら、これらの手段を、CPU11を用いることなく、論理回路などのハードウェア回路のみで構成することも可能であるし、ソフトウェアとハードウェアとの混在により実現することも可能である。

【0035】尚、EEPROM13にキー3に固有の暗号キーを書き込むには、エンジン制御ユニット2に換えて、パーソナルコンピュータなどの外部書込手段28を接続し、通信インターフェース14及びCPU11を介して、EEPROM13の書込を行う。トランスポンダ20のEEPROM24の書込に関しては、イモビライザ10のEEPROM13を書き込むのと同じように外部書込手段28をイモビライザ10に接続し、イモビライザ10からの無線信号でEEPROM24の書込を行う。

【0036】本実施の形態1においては、イモビライザ10の電源オンからエンジンが始動するまでの時間である始動時間データを基に乱数データを生成し、その乱数データを基にキー3の固有情報を暗号化することにより認証キー及び認証コードを生成し、この認証キー及び認証コードを用いてキーの認証を行っている。イモビライザ10の電源オンからエンジンが始動するまでの時間は、エンジンが始動する毎に異なっており、それを予想したり制御することはほとんど不可能である。このため、この始動時間データを基に生成された乱数データは、推測困難で再現性が無く、この乱数を用いた認証はより信頼性の高いものとなる。

【0037】また、始動時間データをEEPROM13に記憶しておき、次にエンジンを始動する時には、EEPROM13にあらかじめ記憶されている始動時間データを基に乱数データを生成している。このため、エンジン停止中の車両に対してより確実な盗難防止が可能である。

【0038】また、エンジンが始動したかどうかの情報のみをエンジン制御ユニット2から受け取ることで始動時間データを生成することができ、エンジン制御ユニット3が出力しなければならない情報は1つだけであり、高性能で高価なエンジン制御ユニット3を必要とせず、エンジン制御ユニット3の負担を軽減し、特にエンジン制御ユニット3が簡易な自動二輪車や原動機付き自転車などの二輪車に有効である。

【0039】また、エンジンの始動により無線部15を停止すると共に、イモビライザ10を休止していることから、エンジン始動後のイモビライザ10の誤動作を防止できると共に、エンジン停止などのエンジンの誤動作を防止できる。

【0040】（実施の形態2）図5は本発明のイモビライザの第2の実施例を示す構成図である。図6は図5のイモビライザの動作の様子を示す構成図である。図7は図5のイモビライザの動作を示すフローチャートであ

る。

【0041】図5～図7において、イモビライザ30は、自動二輪車や原動機付き自転車などの車両のキー3に内蔵されたトランスポンダ20との間で無線通信を行い、トランスポンダ20から送られる情報を基に、キー3がその車両固有のものであるかどうかを識別し、車両の盗難を防止するための装置である。イモビライザ30は、CPU（central processing unit）31、電源部12、EEPROM（Electrically Erasable and Programmable Read Only Memory）13、通信インターフェース34、無線部35により構成されている。

【0042】通信インターフェース34は、CPU31とエンジン制御ユニット28が通信するための仲介役であり、両者間の信号レベルや信号形式を整合させるものである。信号レベルや信号形式については、実施の形態1と同様である。

【0043】無線部35は、CPU11から送られてくる情報を変調するものであり、変調された無線信号は、キーリング4に内蔵されたアンテナ6からトランスポンダ20のアンテナ25に送られる。また、無線部15は、トランスポンダ20から送信された無線信号を、アンテナ6で受信して復調し、復調した情報をCPU31に送る。尚、EEPROM13、電源部12及びトランスポンダ20については、実施の形態1と同様なので説明を省略する。

【0044】次に、イモビライザ30の動作を説明する。尚、以下の説明において、括弧内の符号は図7のフローチャートの符号に対応している。運転者がキー3を用いて車両を始動させようとする場合は、まず、運転者はキー3をキーリング4に挿入する。そして、キー3を運転位置（オン位置）に回す。すると、イグニッションスイッチ5がオンして、電源部12にバッテリー7が接続される。そして、VDD17が電源部12から出力され、イモビライザ30が動作を開始する。

【0045】イモビライザ30が動作を開始すると、CPU31はEEPROM13に格納されている電源オン時間データを読み出す（S202）。尚、電源オン時間データは、イモビライザ30の動作開始からイモビライザ30が電源オフまでの時間を計時手段31aで計時して生成したデータであり、前回イモビライザ30を動作させた時の電源オン時間データが、あらかじめEEPROM13に記憶されている。電源オン時間データの生成のタイミング等は後述する。また、車両を生産して初めてエンジンを始動させる時点でEEPROM13に記憶されているデータは、時間0のデータである。

【0046】次に、CPU11は乱数発生手段31bにより、読み出した電源オン時間データを基に、乱数データを発生させる（S203）。発生させる乱数データの大きさは、例えば10桁である。そして、CPU31は送信データ生成手段31cにより、無線部35からトラ

11

ンスポンダ20に送信するための送信データを生成する(S204)。この送信データ生成手段31cを介することなく、乱数データを直接無線部35から送信させることは可能である。しかしながら、本実施の形態2においては、乱数データに直轄を限定するための情報を付加して、送信データを生成している。すなわち、例えば直轄を限定するための2桁のパスワードを乱数データの先頭に付け加えている。パスワードの機能・効果については後述する。そして、生成された送信データを無線部15からトランスポンダ20に送信する(S205)。

【0047】トランスポンダ20側では、イモビライザ30からの送信データをアンテナ25を介して無線部22で受信する(S251)。無線部22で復調されたパスワード+乱数データを基に、認証キー生成IC23内の認証キー生成手段23aにより、認証キーを生成する(S252)。認証キーは、EEPROM24に記憶されているキー3固有の情報である暗号キーを用いて、乱数データを暗号化したもので、例えば、24ビットのデータである。尚、暗号化の方法は特に限定されるものではなく、例えばDES(Data Encryption Standard; 1977年米国商務省標準局が制定)等の方式が使用可能である。トランスポンダ20は、生成した認証キーを無線部22及びアンテナ25を介してイモビライザ30に送信する(S253)。

【0048】トランスポンダ20の認証キー生成手段23aは、イモビライザ30の情報を受信するとすぐに動作するのではなく、まず、パスワードの内容が、認証キーの生成を行ってもよいものであるかを確認する。当然、不正なパスワードであったり、パスワードがはじめから含まれていない場合には、トランスポンダ20は認証キーの生成及び送信を行わない。このように、トランスポンダ20側からの認証キーの発信を制限することで、このキー3が他車種のイモビライザに接近した場合に、不必要な信号を発信しないようにすることができ、複数のキーを1つのキーホルダに兼ねている場合などに、他車両の正規な認証に混信を与えるのを防止可能である。

【0049】トランスポンダ20は電池を有しておらず、イモビライザ30の無線部35から、パスワード+乱数データの前に送られる電力信号により、無線部22を動作させると共に、コンデンサ21を充電する。すなわち、コンデンサ21は、イモビライザ30の無線部35から送られる電力信号により、2次電池として充電され、トランスポンダ20を動作させる。

【0050】トランスポンダ20が認証キーを生成している間に、イモビライザ30側では認証コードの生成を、CPU31の認証コード生成手段31dにおいて行う(S206)。認証コードは、パスワード+乱数データを基に、EEPROM13に記憶されているキー3固有の情報である暗号キーを用いて、乱数データを暗号化

(7)

特開2001-12123

12

したものである。尚、暗号化の方式は、トランスポンダ20で使用されているものと同一のものである。

【0051】次に、イモビライザ30は、トランスポンダ20からの認証キーを受信する(S207)。そして、CPU31の認証手段31eにおいて、認証コードと認証キーの比較認証を行う(S208)。認証コードと認証キーとが一致した場合には、エンジン始動許可信号を発生する。このエンジン始動許可信号はCPU31から、通信インターフェース34を介して、エンジン制御ユニット2に送られる(S209)。エンジン始動許可信号を受信したエンジン制御ユニット2は、エンジン始動制御2aを行いエンジンを始動させる。実際の自動車や自動二輪車等においては、エンジン始動許可信号によりエンジン始動可能状態となり、運転者のスタータスイッチ(スタートスイッチ)のオンにより、エンジンの始動が行われる。

【0052】その後、イモビライザ30は、10分経過毎にEEPROM13に納められている電源オン時間データを計時手段31aにより1加算してEEPROM13に格納する(S211)。すなわち、イモビライザ30が動作する毎に、動作している時間に見合った数値が足されることになる。尚、加算の間隔は10分としたがこれに限られるものではなく、任意に定められるものである。イグニッションスイッチ5をオフすれば、イモビライザ30の動作は停止し、同時に電源オン時間データの加算変更を停止される。尚、本実施の形態2では、前回イモビライザ30を動作させて時の電源オン時間データに、現在の動作時間を引き続き加算しているがこれに限られるものではなく、認証終了後に一過電源オン時間データを消去してしまい新たに計時を始めてもよい。

【0053】また、本実施の形態2において、計時手段31a、乱数発生手段31b、送信データ生成手段31c、認証コード生成手段31d及び認証手段31eは、CPU31によりソフトウェアとして実現されている。しかしながら、これらの手段を、CPU31を用いることなく、論理回路などのハードウェア回路のみで構成することも可能であるし、ソフトウェアとハードウェアとの混在により実現することも可能である。尚、EEPROM13にキー3に固有の暗号キーを書き込む方法は、実施の形態1と同様のため説明を省略する。

【0054】本実施の形態2においては、イグニッションスイッチ5のオン/オフによりイモビライザ30の電源のオン/オフを行い、イモビライザ30の電源がオンされている時間を電源オン時間データとしており、この電源オン時間データを用いてキーを認証している。イモビライザ30が電源オンしている時間は、車両の運転毎に異なっており、それを予想したり制御することはほとんど不可能である。このため、この電源オン時間データを基に生成された乱数は、推測困難で再現性が無く、この乱数を用いた認証はより信頼性の高いものとなる。

50

(8)

特開2001-12123

13

【0055】また、エンジン制御ユニット2から情報を得なくとも、キー3の認証が可能であることから、新たにエンジン制御ユニット2を設計し直す必要が無く、盗難防止装置としてのコストを抑えることができる。また、既に販売され、使用されている車両に対しても、エンジン制御ユニット2の機能に左右されることなく、容易にイモビライザ30の装着ができる。

【0056】

【発明の効果】請求項1の発明によれば、イモビライザの電源オンからエンジンが始動するまでの時間である始動時間データを基に乱数を生成し、その乱数を基にキーの固有情報を暗号化することにより認証キー及び認証コードを生成し、この認証キー及び認証コードを用いてキーの認証を行っている。イモビライザの電源オンからエンジンが始動するまでの時間は、エンジンが始動する毎に異なっており、それを予想したり制御することはほとんど不可能である。このため、この始動時間データを基に生成された乱数は、推測困難で再現性が無く、この乱数を用いた認証はより信頼性の高いものとなる。また、始動時間データを記憶手段に記憶しておき、次にエンジンを始動する時には、記憶手段にあらかじめ記憶されている始動時間データを基に乱数を生成している。このため、エンジン停止中の車両に対してより確実な盗難防止が可能である。また、エンジンが始動したかどうかの情報のみをエンジン制御ユニットから受け取ることによって始動時間データを生成することができるため、エンジン制御ユニットが出力しなければならない情報は1つだけであり、高性能で高価なエンジン制御ユニットを必要とせず、エンジン制御ユニットの負担を軽減し、特にエンジン制御ユニットが簡易な自動二輪車や原動機付き自転車などの二輪車に有効である。

【0057】請求項2記載の発明によれば、エンジンの始動により無線部を停止すると共に、イモビライザを休止していることから、エンジン始動後のイモビライザの誤動作を防止できると共に、エンジン停止などのエンジンの誤動作を防止できる。

【0058】請求項3の発明によれば、イグニッションスイッチのオン/オフによりイモビライザの電源のオン/オフを行い、イモビライザの電源がオンされている時間を電源オン時間データとしており、この電源オン時間データを用いてキーを認証している。イモビライザが電源オンしている時間は、車両の運転毎に異なっており、それを予想したり制御することはほとんど不可能である。このため、この電源オン時間データを基に生成された乱数は、推測困難で再現性が無く、この乱数を用いた認証はより信頼性の高いものとなる。また、エンジン制御ユニットから情報を得なくとも、キーの認証が可能であることから、新たにエンジン制御ユニットを設計し直す必要が無く、盗難防止装置としてのコストを抑えることができる。また、既に販売され、使用されている車両

14

に対しても、エンジン制御ユニットの機能に左右されることなく、容易にイモビライザの装着ができる。

【0059】請求項4の発明によれば、計時手段により、イモビライザの電源オンから、エンジンが始動するまでの時間をカウントした始動時間データが生成され、この始動時間データを基に乱数発生部が乱数を生成し、その乱数を基にキーの固有情報を暗号化することにより認証キー及び認証コードを生成し、認証手段が認証コードと認証キーとが一致したときに、エンジン制御ユニットにエンジン始動許可信号を送出する。始動時間データは、エンジンが始動する毎に異なっており、それを予想したり制御することはほとんど不可能である。このため、この始動時間データを基に生成された乱数は推測困難で再現性が無く、この乱数を用いた認証はより信頼性の高いものとなる。また、始動時間データを記憶手段に記憶しておき、次にエンジンを始動する時には、記憶手段に記憶されている始動時間データを基に乱数を生成している。このため、エンジン停止中の車両に対してより確実な盗難防止が可能である。また、エンジンが始動したかどうかの情報のみをエンジン制御ユニットから受け取ることによって始動時間データを生成しているため、エンジン制御ユニットが出力しなければならない情報は1つだけであり、高性能で高価なエンジン制御ユニットを必要とせず、エンジン制御ユニットの負担を軽減し、特にエンジン制御ユニットが簡易な自動二輪車や原動機付き自転車などの二輪車に有効である。

【0060】請求項5の発明によれば、エンジンの始動により無線部を停止すると共に、イモビライザを休止していることから、エンジン始動後のイモビライザの誤動作を防止できると共に、エンジン停止などのエンジンの誤動作を防止できる。

【0061】請求項6の発明によれば、イグニッションスイッチによりオン/オフする電源部を備え、電源部がオンされている時間を電源オン時間データとしており、この電源オン時間データを用いてキーを認証している。イモビライザが電源オンしている時間は、車両の運転毎に異なっており、それを予想したり制御することはほとんど不可能である。このため、この電源オン時間データを基に生成された乱数は、推測困難で再現性が無く、この乱数を用いた認証はより信頼性の高いものとなる。また、エンジン制御ユニットから情報を得なくとも、キーの認証が可能であることから、新たにエンジン制御ユニットを設計し直す必要が無く、盗難防止装置としてのコストを抑えることができる。また、既に販売され、使用されている車両に対しても、エンジン制御ユニットの機能に左右されることなく、容易にイモビライザの装着ができる。

【図面の簡単な説明】

【図1】本発明のイモビライザの第1の実施例を示す構成図である。

(9)

特開2001-12123

15

16

【図2】本発明のトランスポンダの一実施例を示す構成図である。

【図3】図1のイモビライザの動作の様子を示す構成図である。

【図4】図1のイモビライザの動作を示すフローチャートである。

【図5】本発明のイモビライザの第2の実施例を示す構成図である。

【図6】図5のイモビライザの動作の様子を示す構成図である。

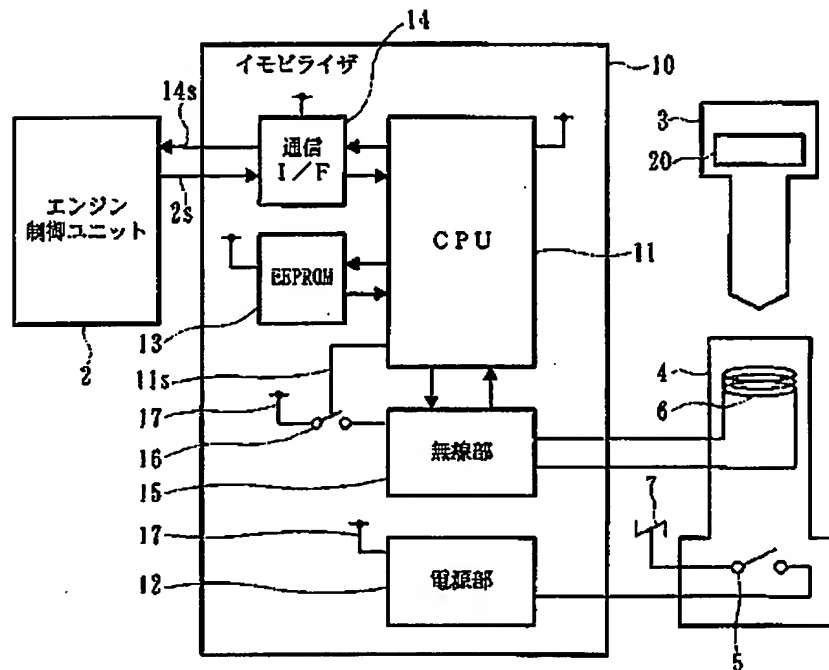
【図7】図5のイモビライザの動作を示すフローチャートである。

【符号の説明】

2. 8 エンジン制御ユニット

* 3 キー
4 キーシリンダ
5 イグニッションスイッチ
6, 25 アンテナ
10, 30 イモビライザ
11, 31 CPU
12 電源部
13, 24 EEPROM
14, 34 通信インターフェース
15, 22 無線部
16 無線部電源スイッチ
20 トランスポンダ
23 認証キー生成IC

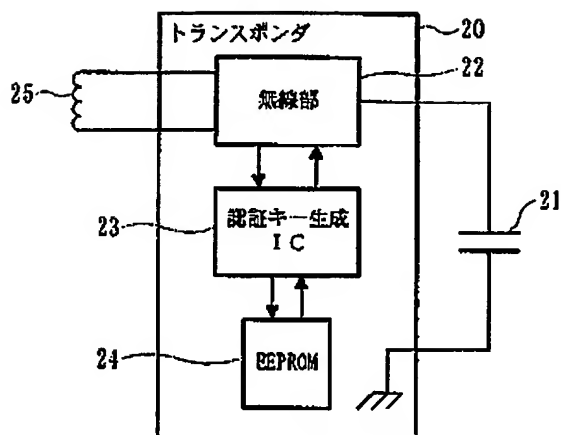
【図1】



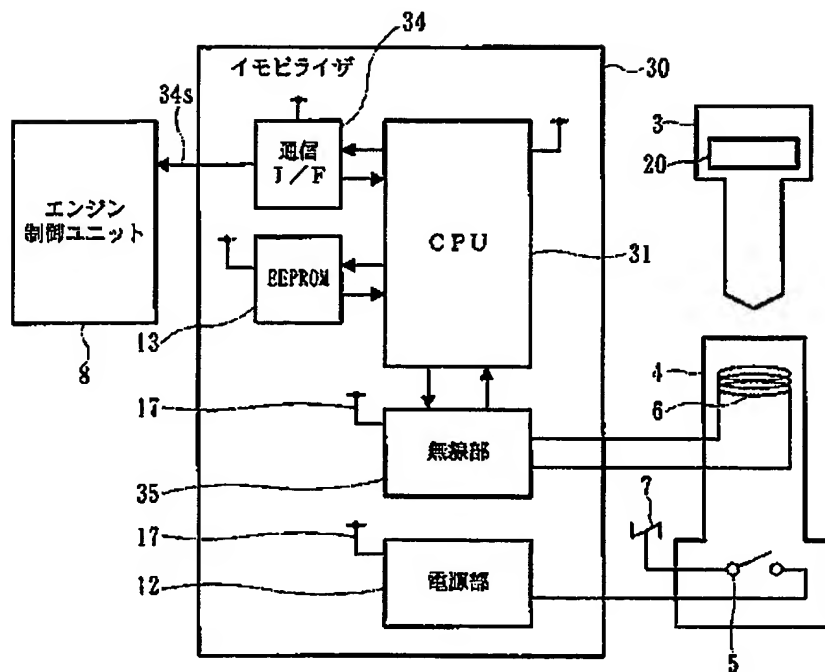
(10)

特開2001-12123

【図2】



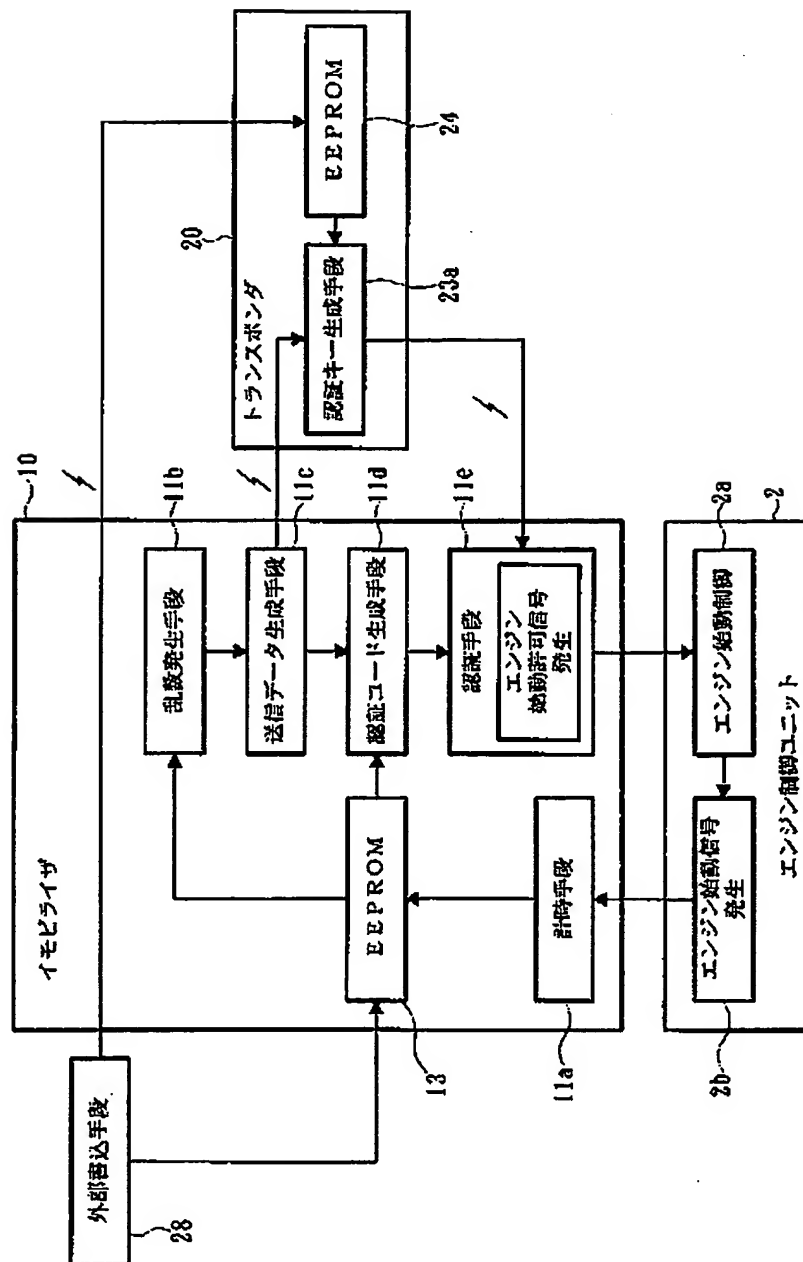
【図5】



特開2001-12123

(11)

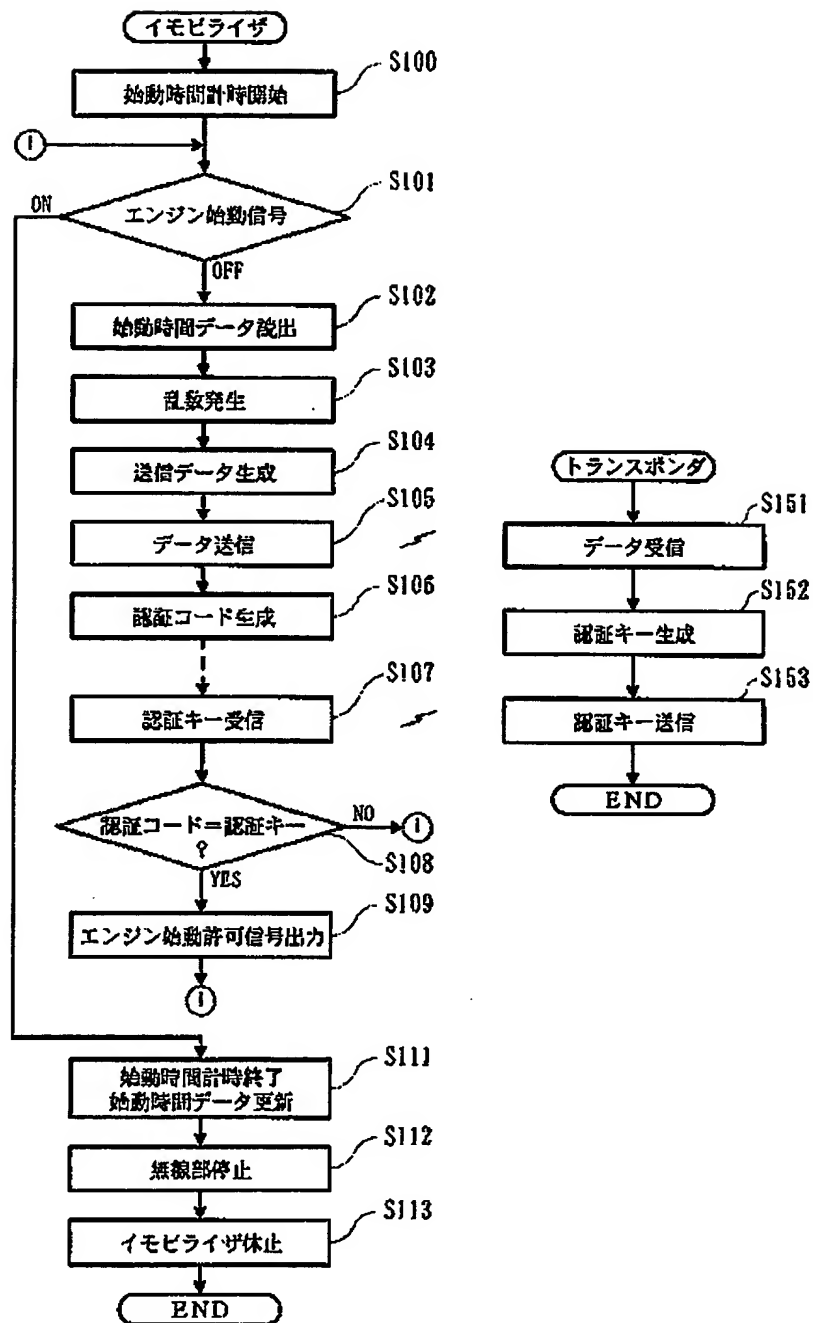
【図3】



(12)

特開2001-12123

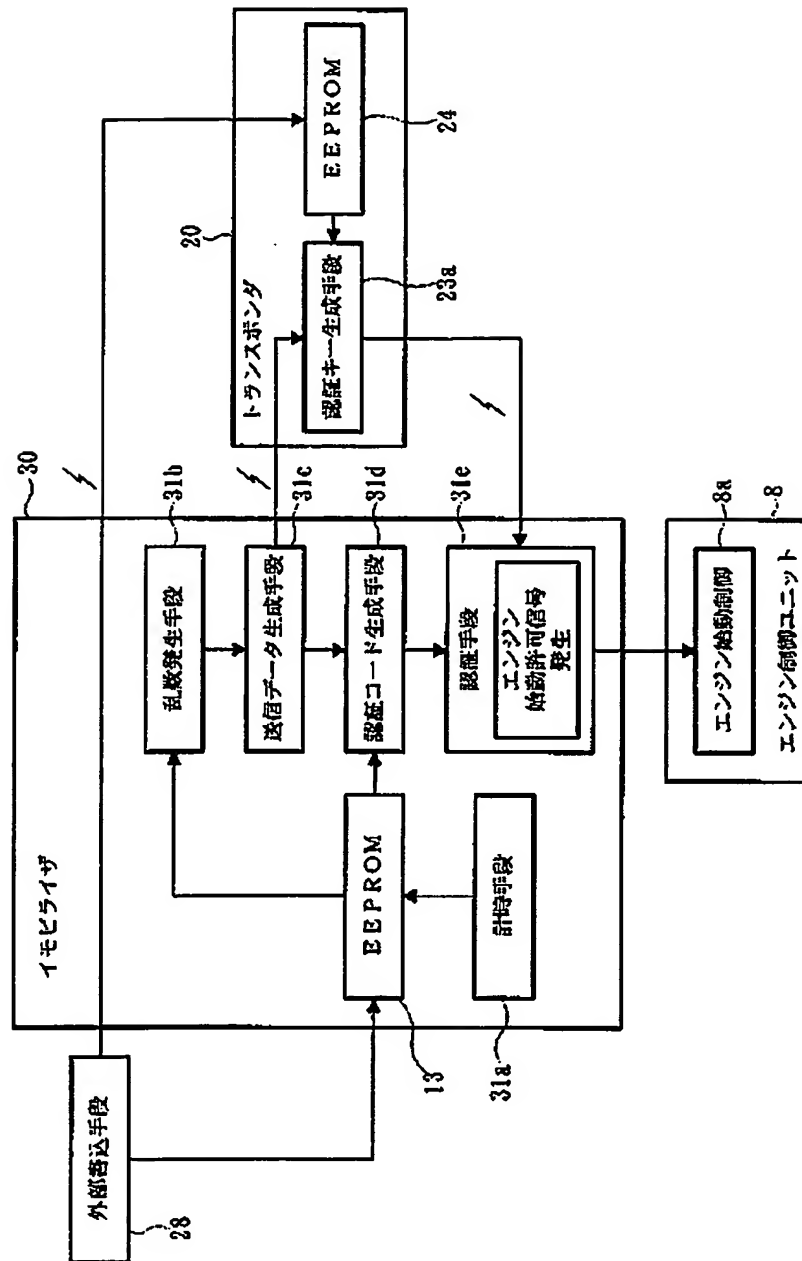
【図4】



(13)

特開2001-12123

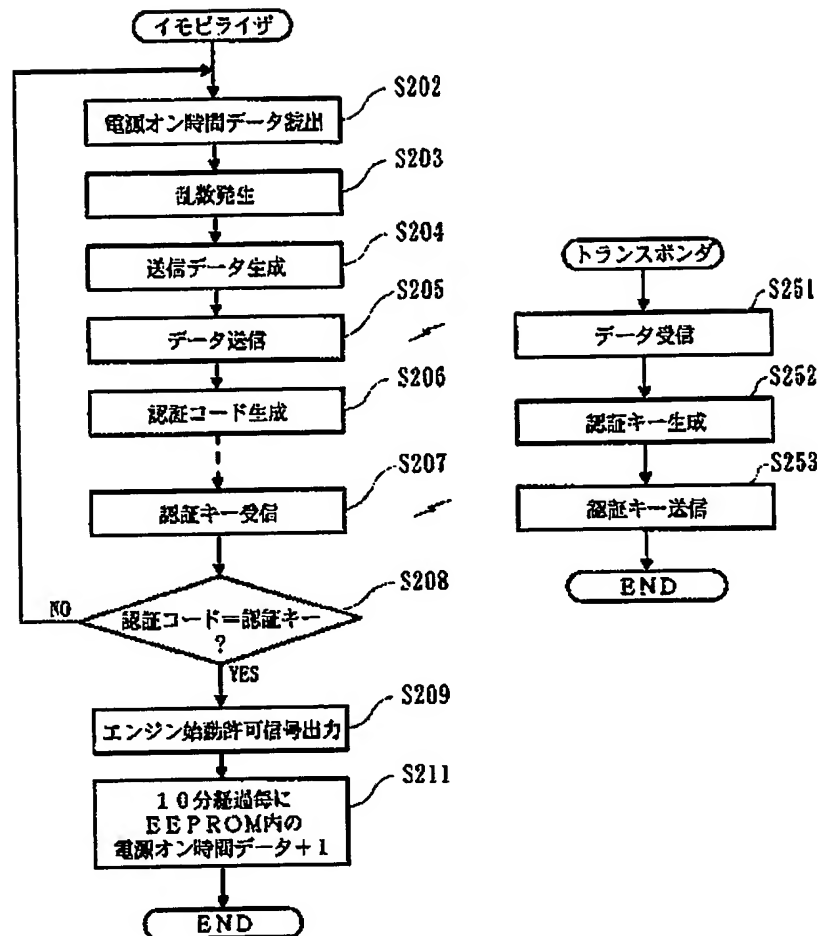
【図6】



(14)

特開2001-12123

【図7】



フロントページの続き

Fターム(参考) 2E250 AA21 BB08 BB56 DD06 EE10
 FF26 FF27 FF36 GG05 HH07
 JJ05 KK03 LL00 PP15 SS04
 TT04
 3G084 BA28 CA01 CA07 DA09 EA07
 EB06 EC04 FA36
 3G093 AA02 BA09 BA26 CA01 DA12
 DA13 DB06 EC01 FA11